

METHOD AND APPARATUS FOR PROVIDING PUBLIC KEY SECURITY CONTROL FOR A CRYPTOGRAPHIC PROCESSOR

Abstract

Public key security control (PKSC) is provided for a cryptographic module by means of
5 digitally signed communications between the module and one or authorities with whom it
interacts. Authorities interact with the crypto module by means of unsigned queries seeking
nonsecret information or signed commands for performing specified operations. Each command
signed by an authority also contains a transaction sequence number (TSN), which must match a
corresponding number stored by the crypto module for the authority. The TSN for each authority
10 is initially generated randomly and is incremented for each command accepted from that authority.
A signature requirement array (SRA) controls the number of signatures required to validate each
command type. Upon receiving a signed command from one or more authorities, the SRA is
examined to determine whether a required number of authorities permitted to sign the command
have signed the command for each signature requirement specification defined for that command
15 type. A command requiring multiple signatures is held in a pending command register (PCR)
while awaiting the required cosignatures. The crypto module also stores a single crypto module
signature sequence number (CMSSN) which it increments for each reply to any authority to
enable one authority to determine whether any other authority has communicated with the
module.